Ransomware Deployment Methods

1. Organisations Under Ransomware Attacks

Please answer the following questions regarding your experience of a ransomware attack. By answering the questionnaire you participate in our research that helps to gain a better understanding of ransomware attacks and thus prevent future incidents. Only statistical information will be gathered from this questionnaire and all participants are kept anonymous. Participation in the questionnaire is voluntary and participants are free to withdraw at any point without prejudice and without providing a reason. All data will be destroyed at the end of the project. We are researchers at The University of Kent undertaking a project called "Ransomware Deployment Methods and Analysis". Should you have any queries or would like to contact us, please do. Henna John hsj4@kent.ac.uk or Gavin Hull gjh9@kent.ac.uk Thank you!

1. I agree to the above statement. *

- [ ] Yes

2. Basic Information

2. What industry does your organisation operate in?

- [ ] Chemical
- [ ] Computer
- [ ] Construction
- [ ] Education
- [ ] Entertainment
- [ ] Financial Services
- [ ] Food
- [ ] Healthcare
- [ ] Hospitality
- [ ] Manufacturing
- [ ] Mass Media
- [ ] Telecommunications
- [ ] Transport
- [ ] Other (please specify):

3. Has your organisation been under a ransomware attack? *

- [ ] Yes
- [ ] No

3. Basic Attack Information

4. When did the latest attack take place (approx.)? *

DD/MM/YYYY

5. What operating system(s) were the infected device(s) or machine(s) running?

- [ ] Windows 10
- [ ] Windows 8
- [ ] Windows 7
- [ ] Windows XP
- [ ] MacOS
- [ ] Linux
- [ ] FreeBSB
- [ ] Android
- [ ] iOS
- [ ] Other (please specify):

6. How did the ransomware first get on the network? *

- [ ] User clicked a link in an email
- [ ] User clicked a link on a website
- [ ] User opened an attachment in an email
- [ ] User attached an unknown device e.g. USB stick to the device
- [ ] User downloaded some software or a binary file
- [ ] Malicious file was downloaded through a sharing network, e.g. peer-to-peer, torrents...
- [ ] Malware exploited a vulnerable part or weakness of the machine
- [ ] Other (please specify):

4. Malicious Link in an Email

7. Who was the sender identified as?

- [ ] Colleague
- [ ] Official authority
- [ ] Other official (e.g. bank, tax, gas)
- [ ] Applicant (job/studies)
- [ ] Other person from recipient's contact list
- [ ] Other (please specify):

8. Sender's email address:

9. Describe the contents of the message:

10. What browser was used to open the link in the email?

11. What website did the link direct to?

5. Malicious Attachment in an Email

12. Who was the sender identified as?

- [ ] Colleague
- [ ] Official authority
- [ ] Other official (e.g. bank, tax, gas)
- [ ] Applicant (job/studies)
- [ ] Other person from recipient's contact list
- [ ] Other (please specify):

13. Sender's email address:

14. Describe the contents of the message:

15. State the type of the attachment (e.g. .doc, .xlsx):

16. How did the malware spread from the file?

- [ ] File had a hidden .exe extension and executed when opened
- [ ] Malware was hidden in file macros
- [ ] Attachment to a DLL or an active process
- [ ] User clicked and activated the file
- [ ] Downloaded other binaries that enabled activation
- [ ] Remotely activated from a C&C server
- [ ] Other (please specify):

6. Malicious Link

17. What browser was used?

18. What website was the malicious link on?

19. What website was the malicious link on?

7. Malicious Software

20. Name the software that was downloaded:

21. What website was the software downloaded from?

22. Was the software part of a bundled package?

- [ ] Yes
- [ ] No

8. File Sharing Network

23. Describe the attacked file sharing network:

9. Vulnerability Exploit

24. Describe the vulnerability that was exploited:

10. More Attack Details

25. From whom did the attack start? *

- [ ] Registered user
- [ ] Guest/Temporary user
- [ ] Intruder
- [ ] Unknown
- [ ] Other (please specify):

26. Was the user using an account with admin privileges at the time of the attack? *

- [ ] Yes
- [ ] No
- [ ] Unknown

27. If yes, why did the user have admin privileges?

28. What type of device was first attacked? *

- [ ] Organisation owned device
- [ ] Personal device
- [ ] Unknown
- [ ] Other (please specify):

29. How was the infected device connected to the network/Internet?

- [ ] WiFi
- [ ] Bluetooth
- [ ] LAN
- [ ] WAN
- [ ] Other (please specify):

30. How many devices were infected during the attack? *

31. How did the malware propagate through the network? (If multiple devices infected)

32. If any, name all internet or endpoint security software running at the time of the attack:

11. More Attack Details

33. What were the first signs of the device(s) being infected?

- [ ] Starting up took much longer than usual
- [ ] Antivirus software was disabled, or took longer to start up
- [ ] Office software, such as MS Word, Excel, etc., crashed, or failed to open files
- [ ] Some files went missing
- [ ] System restarted without consent
- [ ] Screen or display started to jitter
- [ ] Computer started to overheat and became very slow
- [ ] Desktop was locked
- [ ] Computer crashed
- [ ] Indiscriminate or unsolicited communication over the Internet
- [ ] Browser window pop-ups
- [ ] Intrusion Detection System sent alerts about connections to blacklisted IP addresses, vulnerable ports, or suspicious DNS queries
- [ ] Other (please specify):

34. What was the effect of the attack? *

- [ ] Screen blocked
- [ ] Files encrypted
- [ ] Files removed
- [ ] Data stolen
- [ ] MBR / MFT corrupted
- [ ] Other (please specify):

35. What was the name of the ransomware used? (Can often be seen in the extension of encrypted files)

36. How long were the files and/or device(s) locked? *

- [ ] Hours
- [ ] Days
- [ ] Weeks

37. Were you able to recover the files and/or access to the device(s)? *

- [ ] Yes
- [ ] No

12. Files Recovered

38. How were the files and/or access to the device(s) recovered?

- [ ] Ransom was paid
- [ ] Data was recovered from backup
- [ ] Relevant authorities were contacted for advice
- [ ] Reverse engineering
- [ ] Other (please specify):

13. Files Not Recovered

39. What was the reason for not being able to recover the files?

- [ ] Ransom was not paid, and it was not possible to recover files or gain access
- [ ] Ransom was paid, but the attackers did not provide the decryption key or method to unlock the device
- [ ] Ransom was paid, but the decryption key or method to unlock device did not successfully recover files or access to the device
- [ ] Other (please specify):

14. Further Study

We are interested in hearing more details about your organisation's experience with ransomware, and would like to contact you with further questions. This would be very beneficial for the quality of our research. If you are willing to participate in a brief interview, fill in your email address below. Note! No personal information will be stored and all data will be kept anonymous.

40. Email address (optional):